FIG. 1

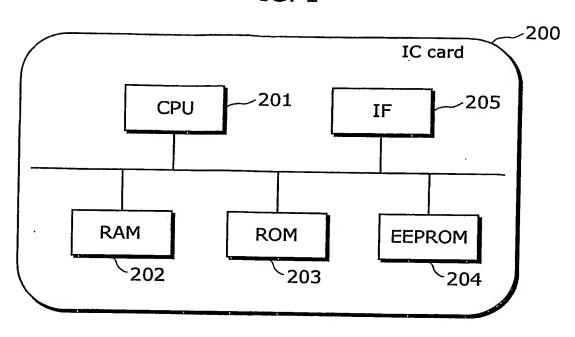


FIG. 2

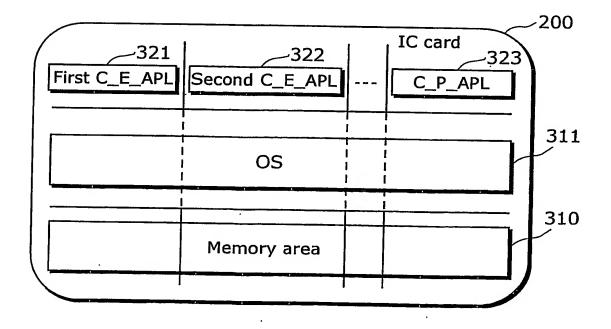


FIG. 3

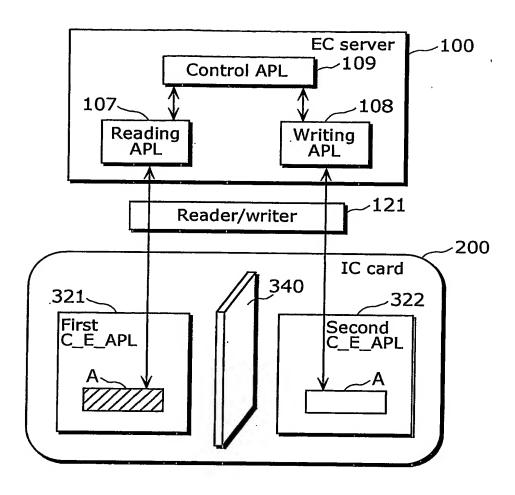


FIG. 4

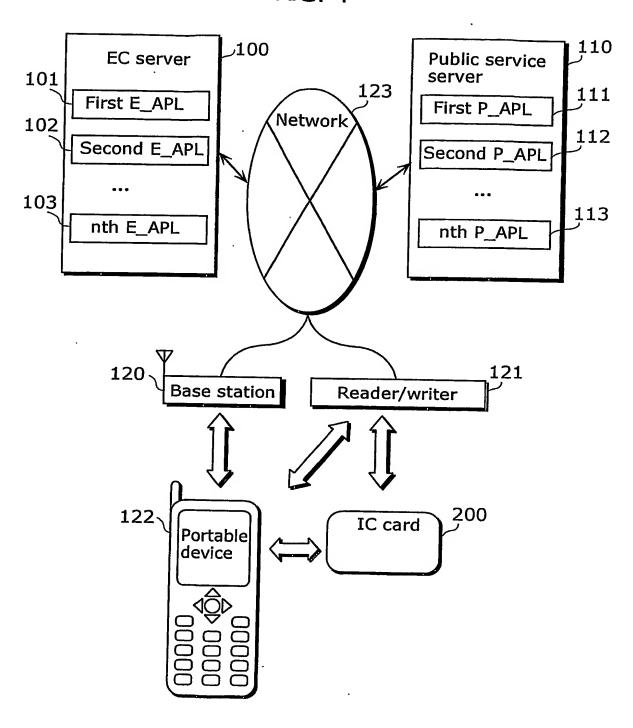


FIG. 5

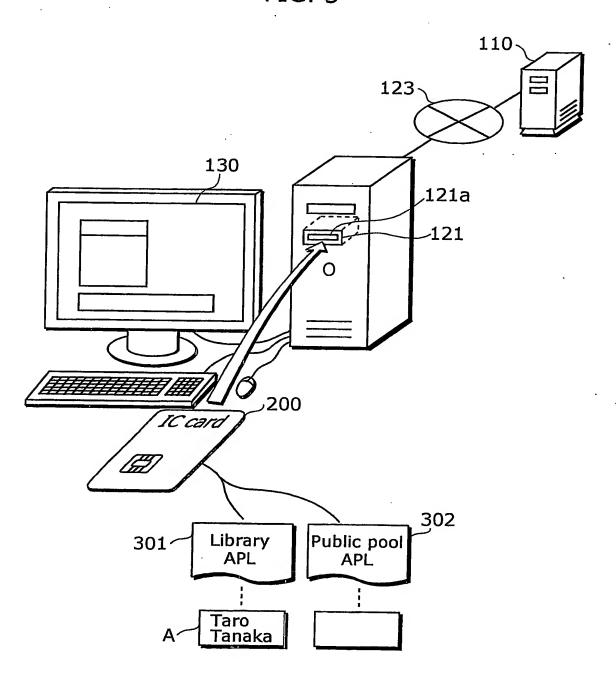
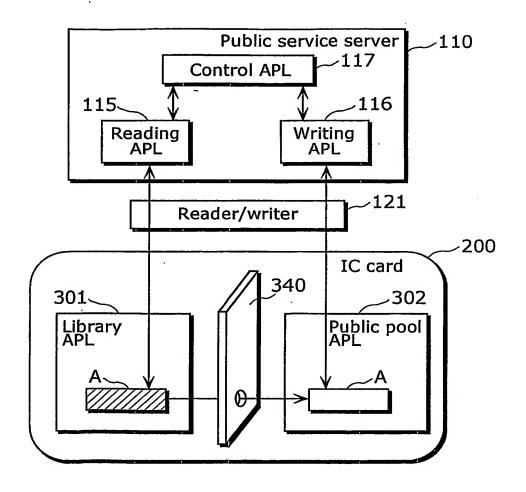


FIG. 6



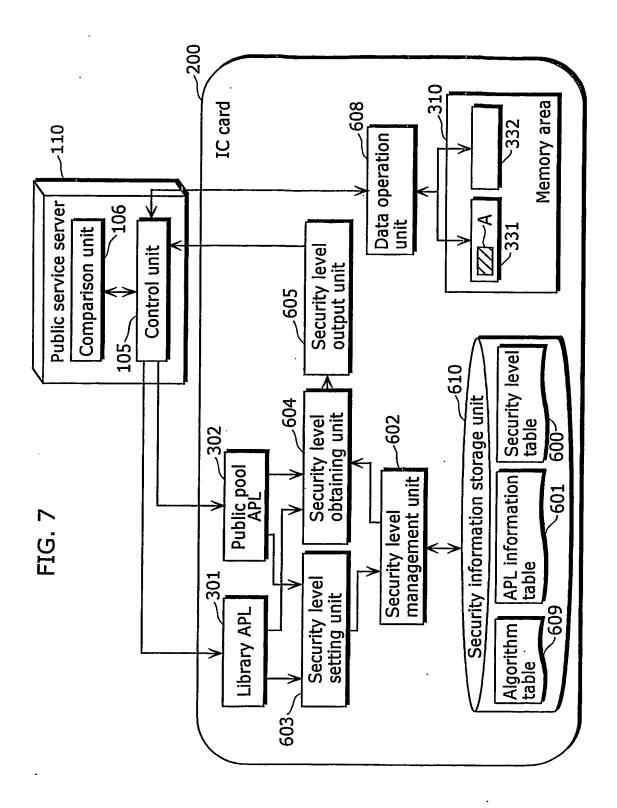


FIG. 8

600ر

Security level table							
Level	Level Value Encryption algorithm						
Strong	03h	Triple-DES					
Medium	02h	DES					
Weak	01h	AES					
None	00h	No encryption					

FIG. 9

609ر

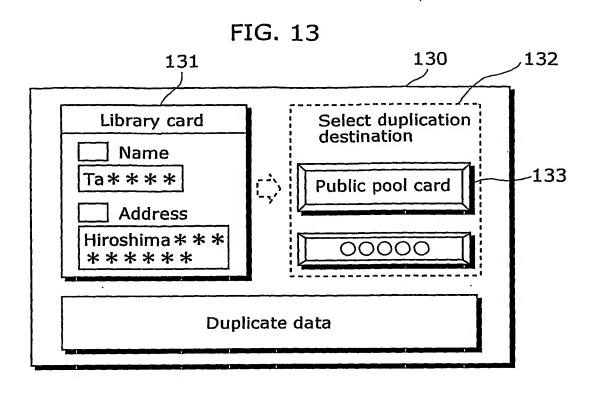
Algorithm table							
Number Encryption algorithm							
0	Triple-DES						
1	DES						
2	AES						
3	No encryption						

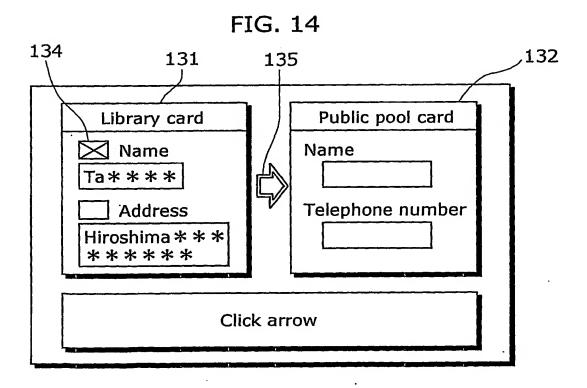
FIG. 10

601								
APL information tab	APL information table							
	, / /							
Library APL information	أمرمر	Application ID	2 bytes					
Public pool APL	, ,	Security level	2 bytes					
information		Encryption information	4 bytes					
•••		Key information	32 bytes					
Electronic money APL information		Protocol version information	4 bytes					

			00h				٠	400					i	00h	
			400					400		_				00h	
		00h	•••	00h			00h		00h				00h	•••	400
		400	03h	00h			00h	FDh	00h				00h	33h	400
.34h	00h	02h	02h	400	78h	00h	400	뜐	00h		FFh	00h	400	22h	00h
12h	01h	80h	01h	01h	56h	03h	COh	FFh	05h		FEh	03h	COh	11h	1Ah
Application ID	Security level	Encryption information	Key information	Version information	Application ID	Security level	Encryption information	Key information	Version information		Application ID	Security level	Encryption information	Key information	Version information
FIG. 11		Library APL			Public pool APL jinformation				•			Electronic money APL information			

FIG. 12 Start S901 Authenticate first APL S902 Authenticate second APL S903 Accept selection of data to be duplicated S904 Obtain security level information S905 Output security level information S906 Security level of first APL ≦ Security level of N second APL? S907 S909 Duplicate data via server Duplicate data inside card S908 Another duplication is to be performed continuously? $N \downarrow$ End





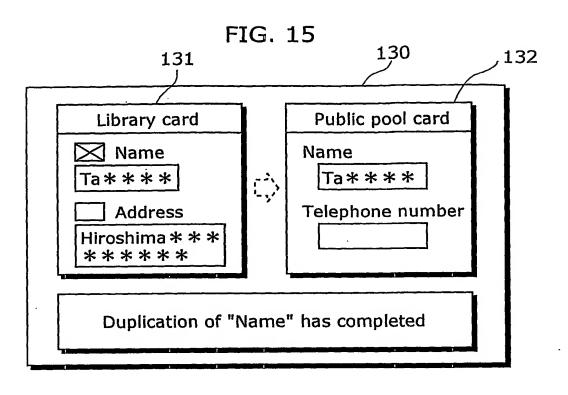
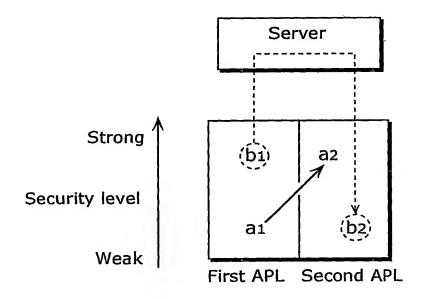
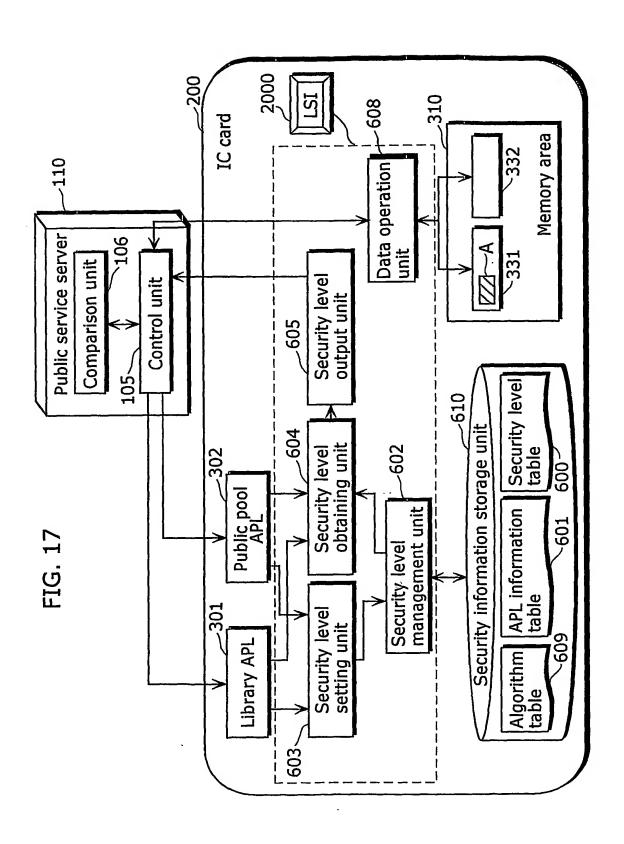
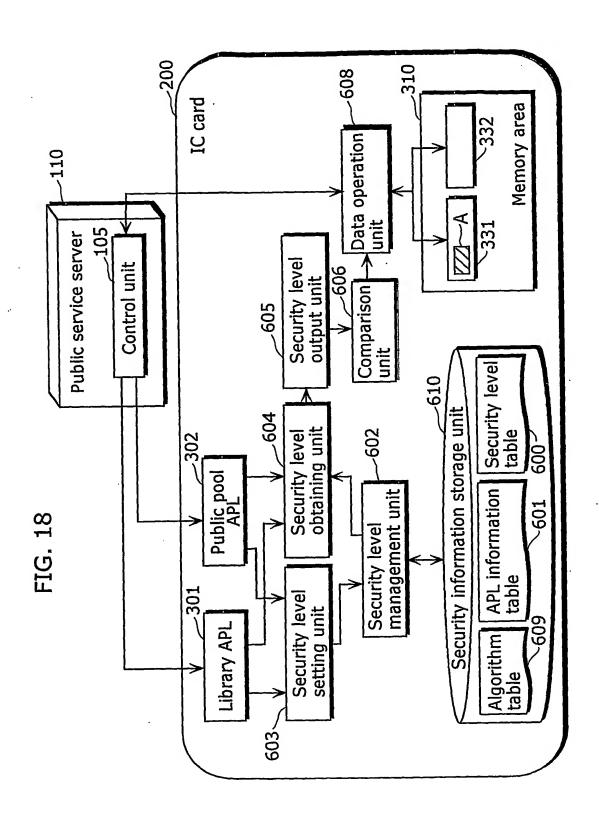


FIG. 16

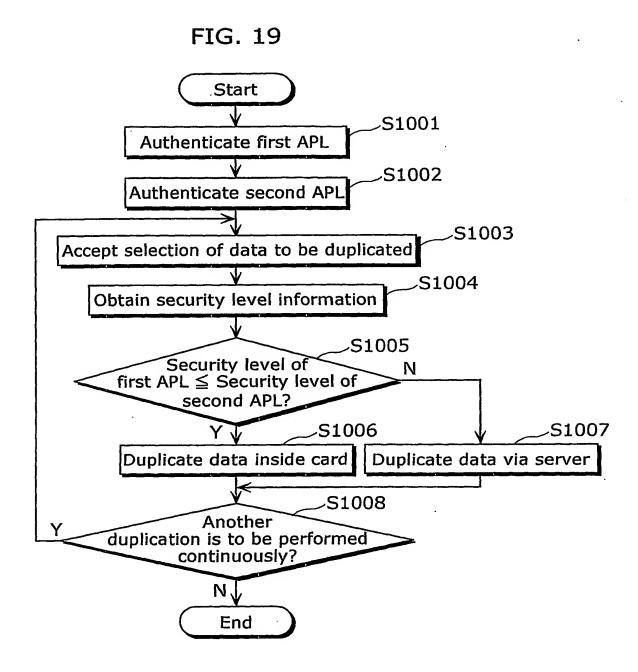




PCT/JP2005/006805



PCT/JP2005/006805



PCT/JP2005/006805

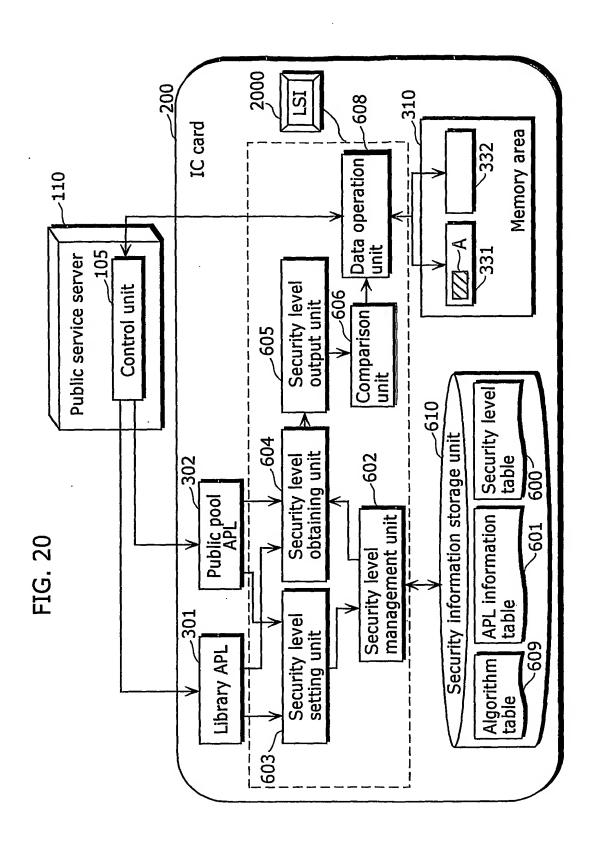


FIG. 21

CLA	INS	P1	P2	Γċ	Data	Le
←—Ma	andato	ry head	ler >	<	Conditional body	/>

FIG. 22

Command name	SELECT	READ RECORD	INTERNAL AUTHENTICATE		
CLA(1byte)	00h	00h	00h		
INS(1byte)	A4h	B2	88h		
P1(1byte)	XXh	Record Number	00h		
P2(1byte)	00h	XXh	00h		

7G. 23

Meaning	Select MF, DF and EF	Select child DF	Select EF under current DF	Select parent DF of current DF	Direct selection by DF name	Select from MF	Select from current DF	Any other value: Not specified
b 1	0	₩.	0	+4	0	0	77	
b2	0	0	Ţ		0	0	0	
b3	0	0	0	0	7	0	0	
b 4	0	0	0	0	0	1	Ţ	
p2	0	0	0	0	0	0	0	
b8 b7 b6 b5 b4 b3 b2 b1	0	0	0	0	0	0	0	
b7	0	0	0	0	0	0	0	
99	0	0	0	0	0	0	0	

FIG. 24

Data section	SW1	SW2
Body	→ Trạ	iler>

FIG. 25

L	8 c	b7	b6	b5	b4	b3	b2	b1	Meaning
	0	0	0	0					Common command
	1	.0	0	0					Unique command

FIG. 26A 200 IC card 202 203 201 205ر **RAM ROM** .CPU IF TRM area Flash Secure 209 memory flash 206 ²⁰⁸ **FeRAM** ²⁰⁷

FIG. 26B

